A recent open source embedded implementation of the DESFire specification designed for on-the-fly logging with NFC based systems

Maxie Dion Schmidt

April 12, 2022

Abstract

Near Field Communication (NFC) is a protocol that offers short-distance wireless communication within a proximity of typically less than 10 centimeters. Embedded NFC tags are common in applications like physical authentication with door readers, university ID cards, bus passes, to exchange credentials renting bikes or motorized scooters, and to charge limited credit transactions to vending machines and other virtual payment kiosks. The Chameleon Mini is a portable device that interfaces with the NFC protocol over RFID. This device is designed to facilitate on-the-fly logging of data exchanges between contactless cards and tag readers operating over NFC in the high-frequency 13.56MHz band. It is an indispensible tool for researchers, reverse engineers and system penetration testers who perform security analysis over the protocol. The Chameleon Mini also supports emulation of many contactless card types over NFC that are enabled by contributions to its open source embedded firmware.

The ability to interface and log low-level exchanges with the popular Mifare DESFire tag type namufactured by Phillips and NXP on the Chameleon Mini is a useful feature to RFID researchers that has been missing from the firmware for many years. In 2020, we set out to offer a fully functional open source implementation to that adds a frequently requested interface to the complex and proprietary DESFire tag command set to the Chameleon Mini RevG firmware. In this technical presentation, we describe the technologies utilized, applications of this work, and describe the challenges of the low-level implementation of the embedded software. Updates to this software project are supported by university COVID-19 relief funding at Georgia Tech over the Spring of 2022.

Keywords: *Near field communication, NFC technology, Chameleon Mini, contactless smartcards, open source software, DESFire command set, RFID cryptographic protocols, embedded systems firmware, reverse engineering.*